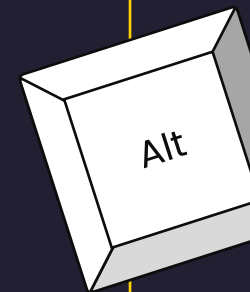
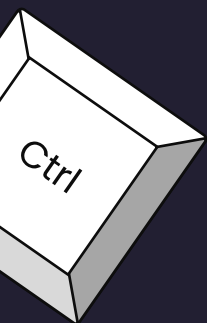


Curated List of Windows Commands for Cybersecurity Analysts



CYBER24X7

Defending 24x7





Contents

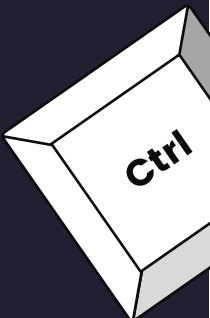
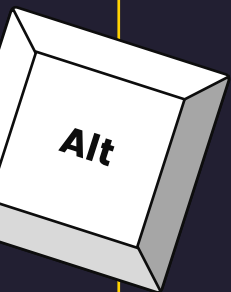
1. System Information & Audit
2. User & Access Investigation
3. Network & Connectivity
4. File System & Integrity
5. Process, Service & Task Analysis
6. Privilege & Security Context
7. Threat Hunting & Live Response
8. Forensics & Artifact Collection
9. System Hardening & Control



CYBER24X7

PART.01

System Information & Audit





Commands for System Information & Audit

Command List

01

systeminfo - Displays detailed system configuration and patch level

02

hostname - Shows the system's hostname

03

whoami - Displays current user and domain

04

net config workstation - Reveals domain, username, and logon server

05

wmic os get Caption,CSDVersion /value - Shows OS version and service pack

06

wmic qfe list - Lists installed Windows updates

07

gpresult /R - Displays applied Group Policies

08

auditpol /get /category:* - Shows audit policy settings

09

wevtutil qe Security /f:text /c:10 - Queries last 10 security log entries

10

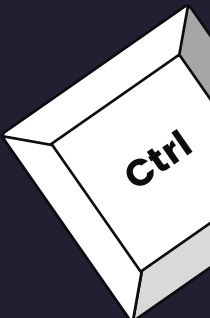
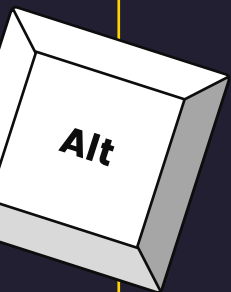
powercfg /energy - Generates a power audit report (can reveal tampering)



CYBER24X7

PART.02

User & Access Investigation





Commands for User & Access Investigation



Command List

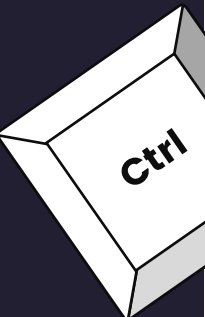
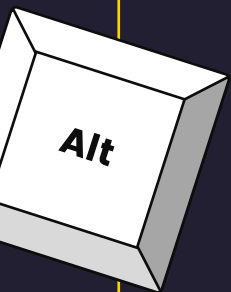
- `net user` - Lists all local users
- `net user [username]` - Shows details of a specific user
- `net localgroup administrators` - Lists local admins
- `query user` - Displays active sessions
- `whoami /groups` - Lists group memberships
- `runas /user:[domain\user] cmd` - Runs command as another user
- `net accounts` - Shows password and lockout policies
- `wmic useraccount get name,sid` - Displays usernames and SIDs
- `dir /b /s C:\Users` - Lists all user directories
- `tasklist /v` - Shows running processes with user context



CYBER24X7

PART.03

Network & Connectivity





Commands for Network & Connectivity



Command List

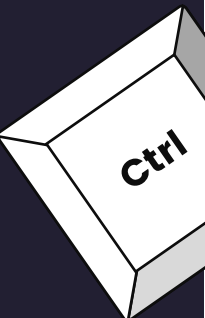
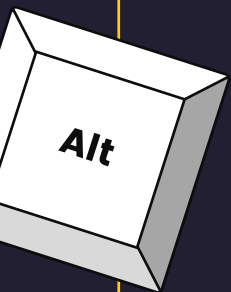
- `ipconfig /all` - Displays full network configuration
- `tracert [domain]` - Traces route to a host
- `netstat - ano` - Lists active connections with PID
- `ping [host]` - Checks connectivity
- `arp - a` - Shows ARP cache (can reveal spoofing)
- `netsh wlan show profiles` - Lists saved Wi-Fi profiles
- `route print` - Displays routing table
- `netsh advfirewall show allprofiles` - Displays firewall status
- `nslookup [domain]` - Resolves DNS queries
- `netsh interface ipv4 show config` - Shows IP settings per interface



CYBER24X7

PART.04

File System & Integrity





Commands for File System & Integrity



Command List

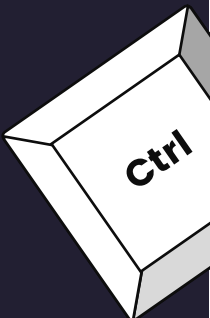
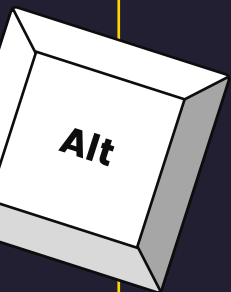
- `dir /s /b` - Lists all files recursively
- `attrib` - Displays file attributes (hidden, system, etc.)
- `icacls [file/folder]` - Shows and modifies ACLs
- `cipher /c /h` - Checks file encryption status
- `fsutil file layout [filename]` - Reveals physical layout of a file
- `findstr /s /i /m "password" *.*` - Searches for sensitive strings
- `tree /f` - Displays folder structure with files
- `type [filename]` - Displays file content
- `fc [file1] [file2]` - Compares two files
- `sfc /scannow` - Scans system files for integrity violations



CYBER24X7

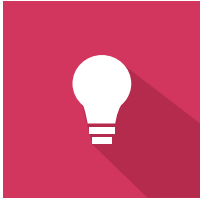
PART.05

Process, Service & Task Analysis





Commands for Process, Service & Task Analysis



Command List

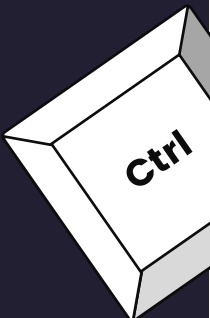
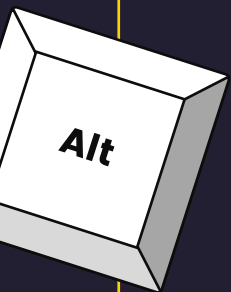
- tasklist - Lists running processes
- taskkill /pid [PID] /f - Forcefully kills a process
- sc query - Lists services and their states
- sc qc [service] - Shows service configuration
- wmic process list brief - Displays process summary
- wmic service get name,startmode,state - Lists services with startup modes
- schtasks /query /fo LIST /v - Lists scheduled tasks
- driverquery - Lists installed drivers
- reg query HKLM\... - Queries registry keys
- reg export - Exports registry for analysis



CYBER24X7

PART.06

Privilege & Security Context





Commands for Privilege & Security Context

Command List

01

whoami /priv - Lists current user's privileges

02

net session - Shows active sessions on the machine

03

net share - Lists shared folders and permissions

04

accesschk.exe - uws [username] *
- Checks user access rights (Sysinternals)

05

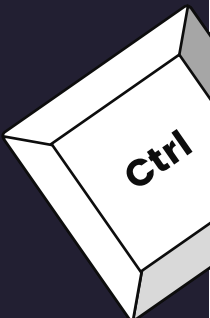
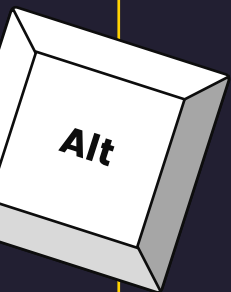
cacls [file] - Legacy ACL viewer (use icacls for modern)



CYBER24X7

PART.07

Threat Hunting & Live Response





Commands for Threat Hunting & Live Response

Command List



wmic startup get
caption,command -
Lists startup
programs



netstat - b - n -
Shows active
connections with
executable names



tasklist /m - Lists
loaded modules per
process



sigcheck.exe - q - m
- c - Verifies digital
signatures
(Sysinternals)



handle.exe - Lists
open handles
(Sysinternals)

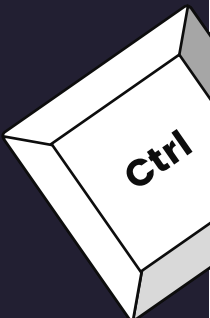
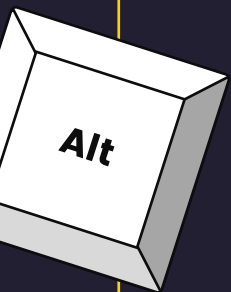




CYBER24X7

PART.08

Forensics & Artifact Collection





Commands for Forensics & Artifact Collection

Command List



`dir /a /s /t:c` - Lists files with creation timestamps



`type %APPDATA%\Microsoft\Windows\Recent\*` - Views recent file access history



`dir /s /b *.lnk` - Finds shortcut files (can reveal staging)



`find /c /i "password" *.txt` - Counts files with keyword matches

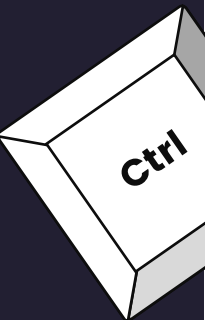
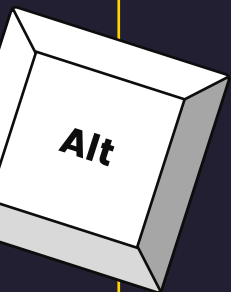


`wmic logicaldisk get name,freespace,size` - Shows disk usage and capacity



PART.09

System Hardening & Control





Commands for System Hardening & Control



Command List



`netsh firewall show state` - Displays firewall status



`gpupdate /force` - Forces Group Policy refresh



`bcdedit` - Views bootloader settings



`schtasks /delete /tn [taskname]` - Deletes scheduled task



`secedit /export /cfg secconfig.cfg` - Dumps local security policy

Thanks



CYBER24X7

Defending 24x7

